Manage SVMs

REST API reference

NetApp
February 06, 2026

Table of Contents

Manage SVMs

Manage SVMs

Managing SVMs

Cluster administrators can manage any SVM bound to the cluster. In addition, SVMs can also be managed by their SVM administrators. The SVM administrator manages the SVM resources, such as volumes, protocols and services, depending on the capabilities assigned by the cluster administrator. SVM administrators cannot create, modify, or delete SVMs. The cluster administrator manages SVM create, modify, or delete operations.

While configuring CIFS, you must also configure IP interfaces and DNS. No other protocol configuration is allowed when configuring NVMe. NFS, FCP, CIFS, iSCSI, and S3 protocols can be configured together.

SVM administrators might have all or some of the following administration capabilities:

1. Data access protocol configuration Configures data access protocols, such as NFS, CIFS, iSCSI, S3, and Fibre Channel (FC) protocols (Fibre Channel over Ethernet included).
2. Services configuration Configures services such as LDAP, NIS, and DNS.
3. Monitoring SVM Monitors jobs, network connections, network interfaces, and SVM health.
4. Updating the TLS certificate for this SVM.

Retrieve SVMs and SVM properties

GET `/svm/svms`

Introduced In: 9.6

Retrieves a list of SVMs and individual SVM properties. This includes protocol configurations such as CIFS, NFS and S3, export policies, name service configurations, and network services.

Important notes

- The SVM object includes a large set of fields and can be expensive to retrieve. Use this API to list the collection of SVMs, and to retrieve only the full details of individual SVMs as needed.
- It is not recommended to create or delete more than five SVMs in parallel.
- REST APIs only expose a data SVM as an SVM.

Expensive properties

There is an added computational cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See Requesting specific fields to learn more.

- `snapmirror.*`

Related ONTAP commands

- `vserver show`

Examples

- Retrieves a list of SVMs in the cluster sorted by name.

```
GET "/api/svm/svms?order_by=name"
```

- Retrieves a list of SVMs in the cluster that have the NFS protocol enabled.

```
GET "/api/svm/svms?nfs.enabled=true"
```

- Retrieves a list of SVMs in the cluster that have the CIFS protocol enabled.

```
GET "/api/svm/svms?cifs.enabled=true"
```

- Retrieves a list of SVMs in the cluster that have the S3 protocol enabled.

```
GET "/api/svm/svms?s3.enabled=true"
```

- Retrieves a list of SVMs in the cluster that have the FCP protocol allowed.

```
GET "/api/svm/svms?fcp.allowed=true"
```

- Retrieves a list of SVMs in the cluster that have the CIFS protocol allowed.

```
GET "/api/svm/svms?cifs.allowed=true"
```

- Retrieves a list of SVMs in the cluster where the NDMP protocol is specified as allowed.

```
GET "/api/svm/svms?ndmp.allowed=true"
```

- Retrieves a list of SVMs in the cluster that have the s3 protocol allowed.

```
GET "/api/svm/svms?s3.allowed=true"
```

Learn more

- DOC /svm/svms

Parameters

Name	Type	In	Required	Description
nis.enabled	boolean	query	False	Filter by nis.enabled
nis.servers	string	query	False	Filter by nis.servers
nis.domain	string	query	False	Filter by nis.domain
nvme.allowed	boolean	query	False	Filter by nvme.allowed • Introduced in: 9.9
nvme.enabled	boolean	query	False	Filter by nvme.enabled
language	string	query	False	Filter by language
nfs.allowed	boolean	query	False	Filter by nfs.allowed • Introduced in: 9.9
nfs.enabled	boolean	query	False	Filter by nfs.enabled
comment	string	query	False	Filter by comment
aggregates.name	string	query	False	Filter by aggregates.name
aggregates.uuid	string	query	False	Filter by aggregates.uuid
subtype	string	query	False	Filter by subtype
dns.servers	string	query	False	Filter by dns.servers
dns.domains	string	query	False	Filter by dns.domains
fcp.allowed	boolean	query	False	Filter by fcp.allowed • Introduced in: 9.9

Name	Type	In	Required	Description
fcp.enabled	boolean	query	False	Filter by fcp.enabled
iscsi.allowed	boolean	query	False	Filter by iscsi.allowed • Introduced in: 9.9
iscsi.enabled	boolean	query	False	Filter by iscsi.enabled
name	string	query	False	Filter by name
ipspace.uuid	string	query	False	Filter by ipspace.uuid
ipspace.name	string	query	False	Filter by ipspace.name
ldap.base_dn	string	query	False	Filter by ldap.base_dn
ldap.servers	string	query	False	Filter by ldap.servers
ldap.enabled	boolean	query	False	Filter by ldap.enabled
ldap.bind_dn	string	query	False	Filter by ldap.bind_dn
ldap.ad_domain	string	query	False	Filter by ldap.ad_domain
uuid	string	query	False	Filter by uuid
cifs.name	string	query	False	Filter by cifs.name
cifs.ad_domain.fqdn	string	query	False	Filter by cifs.ad_domain.fqdn
cifs.ad_domain.organizational_unit	string	query	False	Filter by cifs.ad_domain.organizational_unit

Name	Type	In	Required	Description
cifs.allowed	boolean	query	False	Filter by cifs.allowed • Introduced in: 9.9
cifs.enabled	boolean	query	False	Filter by cifs.enabled
s3.name	string	query	False	Filter by s3.name • Introduced in: 9.7
s3.allowed	boolean	query	False	Filter by s3.allowed • Introduced in: 9.12
s3.enabled	boolean	query	False	Filter by s3.enabled • Introduced in: 9.7
s3.is_http_enabled	boolean	query	False	Filter by s3.is_http_enabled • Introduced in: 9.16
s3.is_https_enabled	boolean	query	False	Filter by s3.is_https_enabled • Introduced in: 9.16
s3.port	integer	query	False	Filter by s3.port • Introduced in: 9.16
s3.secure_port	integer	query	False	Filter by s3.secure_port • Introduced in: 9.16

Name	Type	In	Required	Description
s3.certificate.uuid	string	query	False	Filter by s3.certificate.uuid • Introduced in: 9.16
s3.certificate.name	string	query	False	Filter by s3.certificate.name • Introduced in: 9.16
ndmp.allowed	boolean	query	False	Filter by ndmp.allowed • Introduced in: 9.10
nsswitch.netgroup	string	query	False	Filter by nsswitch.netgroup
nsswitch.group	string	query	False	Filter by nsswitch.group
nsswitch.hosts	string	query	False	Filter by nsswitch.hosts
nsswitch.namemap	string	query	False	Filter by nsswitch.namemap
nsswitch.passwd	string	query	False	Filter by nsswitch.passwd
qos_policy.name	string	query	False	Filter qos_policy.name • Introduced in: 9.9
qos_policy.uuid	string	query	False	Filter qos_policy.uuid • Introduced in: 9.9

Name	Type	In	Required	Description
max_volumes	string	query	False	Filter max_volumes • Introduced in: 9.9
fc_interfaces.name	string	query	False	Filter by fc_interfaces.name • Introduced in: 9.7
fc_interfaces.data_protocol	string	query	False	Filter by fc_interfaces.data_protocol • Introduced in: 9.7
snapshot_policy.uuid	string	query	False	Filter by snapshot_policy.uuid
snapshot_policy.name	string	query	False	Filter by snapshot_policy.name
state	string	query	False	Filter by state
certificate.uuid	string	query	False	Filter by certificate.uuid • Introduced in: 9.7
anti_ransomware_default_volume_state	string	query	False	Filter by anti_ransomware_default_volume_state • Introduced in: 9.10
qos_adaptive_policy_group_template.name	string	query	False	Filter by qos_adaptive_policy_group_template.name • Introduced in: 9.13

Name	Type	In	Required	Description
qos_adaptive_policy_group_template.uuid	string	query	False	Filter by qos_adaptive_policy_group_template.uuid • Introduced in: 9.13
qos_policy_group_template.name	string	query	False	Filter by qos_policy_group_template.name • Introduced in: 9.16
qos_policy_group_template.uuid	string	query	False	Filter by qos_policy_group_template.uuid • Introduced in: 9.16
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	query	False	Filter by anti_ransomware_auto_switch_from_learning_to_enabled • Introduced in: 9.13
anti_ransomware_auto_switch_minimum_incoming_data	string	query	False	Filter by anti_ransomware_auto_switch_minimum_incoming_data • Introduced in: 9.13
anti_ransomware_auto_switch_minimum_incoming_data_percent	integer	query	False	Filter by anti_ransomware_auto_switch_minimum_incoming_data_percent • Introduced in: 9.13

Name	Type	In	Required	Description
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	query	False	Filter by anti_ransomware_auto_switch_duration_without_new_file_extension • Introduced in: 9.13
anti_ransomware_auto_switch_minimum_learning_period	integer	query	False	Filter by anti_ransomware_auto_switch_minimum_learning_period • Introduced in: 9.13
anti_ransomware_auto_switch_minimum_file_count	integer	query	False	Filter by anti_ransomware_auto_switch_minimum_file_count • Introduced in: 9.13
anti_ransomware_auto_switch_minimum_file_extension	integer	query	False	Filter by anti_ransomware_auto_switch_minimum_file_extension • Introduced in: 9.13
auto_enable_analytics	boolean	query	False	Filter by auto_enable_analytics. • Introduced in: 9.12
auto_enable_activity_tracking	boolean	query	False	Filter by auto_enable_activity_tracking. • Introduced in: 9.12

Name	Type	In	Required	Description
storage.allocated	integer	query	False	Filter by storage_allocated • Introduced in: 9.14
storage.available	integer	query	False	Filter by storage_available • Introduced in: 9.14
storage.used_percentage	integer	query	False	Filter by storage_used_percentage • Introduced in: 9.14
number_of_volumes_in_recovery_queue	integer	query	False	Filter by number_of_volumes_in_recovery_queue • Introduced in: 9.13
total_volume_size_in_recovery_queue	integer	query	False	Filter by total_volume_size_in_recovery_queue • Introduced in: 9.13
storage.limit_threshold_exceeded	integer	query	False	Filter by storage.limit_threshold_exceeded • Introduced in: 9.14
storage.limit	integer	query	False	Filter by storage.limit • Introduced in: 9.14

Name	Type	In	Required	Description
storage.limit_threshold_alert	integer	query	False	Filter by storage.limit_threshold_alert • Introduced in: 9.14
snapshot_autodelete_enabled	boolean	query	False	Filter by snapshot_autodelete_enabled • Introduced in: 9.18
snapshot_reserve_percent	integer	query	False	Filter by snapshot_reserve_percent • Introduced in: 9.18
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[svm]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "aggregates": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "available_size": 10156560384,
          "name": "aggr1",
          "snaplock_type": "string",
          "state": "string",
          "type": "string",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      ],
      "anti_ransomware_auto_switch_minimum_incoming_data": "string",
      "anti_ransomware_default_volume_state": "string",
      "anti_ransomware_incoming_write_threshold": "string",
      "anti_ransomware_incoming_write_threshold_percent": "string",
      "certificate": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
```

```
      },
      "cifs": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "ad_domain": {
          "default_site": "string",
          "fqdn": "example.com",
          "organizational_unit": "string"
        },
        "auth-style": "domain",
        "domain_workgroup": "string",
        "name": "CIFS1",
        "workgroup": "workgrp1"
      },
      "comment": "string",
      "dns": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "domains": [
          "example.com",
          "example2.example3.com"
        ],
        "servers": [
          "10.224.65.20",
          "2001:db08:a0b:12f0::1"
        ]
      },
      "fc_interfaces": [
        {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "data_protocol": "string",
          "name": "lif1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      ],
      "fcp": {
```

```
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "ip_interfaces": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "ip": {
          "address": "10.10.10.7"
        },
        "name": "lif1",
        "services": [
          "data_nfs"
        ],
        "subnet": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "subnet1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "ipspace": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "Default",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "iscsi": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
```

```
      }
    },
    "language": "c.utf_8",
    "ldap": {
      "ad_domain": "string",
      "base_dn": "string",
      "bind_dn": "string",
      "servers": [
        "string"
      ]
    },
    "max_volumes": "string",
    "name": "svm1",
    "nfs": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "nis": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "domain": "string",
      "servers": [
        "string"
      ]
    },
    "nsswitch": {
      "group": [
        "string"
      ],
      "hosts": [
        "string"
      ],
      "namemap": [
        "string"
      ],
      "netgroup": [
        "string"
      ],
      "passwd": [
        "string"
```

```
      ]
    },
    "number_of_volumes_in_recovery_queue": 0,
    "nvme": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
    "qos_adaptive_policy_group_template": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "max_throughput_iops": 10000,
      "max_throughput_mbps": 500,
      "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "min_throughput_iops": 2000,
      "min_throughput_mbps": 500,
      "name": "performance",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "qos_policy": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
```

```
      },
      "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "max_throughput_iops": 10000,
      "max_throughput_mbps": 500,
      "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "min_throughput_iops": 2000,
      "min_throughput_mbps": 500,
      "name": "performance",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "qos_policy_group_template": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "max_throughput_iops": 10000,
      "max_throughput_mbps": 500,
      "min_throughput": [
        "900KB/s",
        "500MB/s",
```

```
          "120GB/s",
          "5000IOPS",
          "5000IOPS,500KB/s",
          "2500IOPS,100MB/s",
          "1000IOPS,25MB/s"
        ],
        "min_throughput_iops": 2000,
        "min_throughput_mbps": 500,
        "name": "performance",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "s3": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "certificate": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "string",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "default_unix_user": "string",
        "default_win_user": "string",
        "name": "s3-server-1"
      },
      "snapmirror": {
        "protected_consistency_group_count": 0,
        "protected_volumes_count": 0
      },
      "snapshot_policy": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "state": "running",
      "storage": {
        "allocated": 0,
```

```
        "available": 0,
        "used_percentage": 0
      },
      "subtype": "string",
      "total_volume_size_in_recovery_queue": 0,
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

aggregates

Name	Type	Description
_links	_links	
available_size	integer	Space available, in bytes.
name	string	
snaplock_type	string	SnapLock type.
state	string	Aggregate state.
type	string	Type of aggregate.
uuid	string	

event_log

Name	Type	Description
is_enabled_on_new_file_extension_seen	boolean	Specifies whether to send an EMS when a new file extension is discovered.
is_enabled_on_snapshot_copy_creation	boolean	Specifies whether to send an EMS when a snapshot is created.

arw_vserver

Anti-ransomware related information for the SVM.

Name	Type	Description
event_log	event_log	

certificate

Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server.

cifs

Name	Type	Description
_links	_links	
ad_domain	ad_domain	
allowed	boolean	If this is set to true, an SVM administrator can manage the CIFS service. If it is false, only the cluster administrator can manage the service.

Name	Type	Description
auth-style	string	Authentication type.
domain_workgroup	string	The NetBIOS name of the domain or workgroup associated with the CIFS server.
enabled	boolean	If allowed, setting to true enables the CIFS service.
name	string	The NetBIOS name of the CIFS server.
workgroup	string	The workgroup name.

dns

Name	Type	Description
_links	_links	
domains	array[string]	A list of DNS domains. Domain names have the following requirements: • The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_". • The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9. • The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9. • The top level domain must contain only the following characters: A through Z, a through z. • The system reserves the following names:"all", "local", and "localhost".

Name	Type	Description
servers	array[string]	The list of IP addresses of the DNS servers. Addresses can be either IPv4 or IPv6 addresses.

node

The node on which the FC port is located.

Name	Type	Description
name	string	The name of the node on which the FC port is located.

fc_port_reference

An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

Name	Type	Description
_links	_links	
name	string	The name of the FC port.
node	node	The node on which the FC port is located.
uuid	string	The unique identifier of the FC port.

location

The location of the Fibre Channel interface is defined by the location of its port.

Name	Type	Description
port	fc_port_reference	An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

fc_interface_svm

Name	Type	Description
_links	_links	

Name	Type	Description
data_protocol	string	The data protocol for which the Fibre Channel interface is configured.
name	string	The name of the Fibre Channel interface.
uuid	string	The unique identifier of the Fibre Channel interface.

fcp

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the FCP service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the FCP service.

ip

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address

broadcast_domain

Broadcast domain UUID along with a readable name.

Name	Type	Description
_links	_links	
name	string	Name of the broadcast domain, scoped to its IPspace
uuid	string	Broadcast domain UUID

home_node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

port_svm

Name	Type	Description
_links	_links	
name	string	
uuid	string	

location

Home_node is optional.

Name	Type	Description
broadcast_domain	broadcast_domain	Broadcast domain UUID along with a readable name.
home_node	home_node	
home_port	port_svm	

ip_subnet_reference

A named subnet. Either UUID or name can be supplied on input.

Name	Type	Description
_links	_links	
name	string	The name of the subnet. If only the name is provided, the IPspace scope must be provided by the object this object is embedded in.
uuid	string	The UUID that uniquely identifies the subnet.

ip_interface_svm

Interface parameters. Name and home_node are optional.

Name	Type	Description
_links	_links	
ip	ip	IP information
name	string	The name of the interface (optional).
services	array[string]	The services associated with the interface.
subnet	ip_subnet_reference	A named subnet. Either UUID or name can be supplied on input.
uuid	string	The UUID that uniquely identifies the interface.

ipspace

Either the UUID or name may be supplied on input.

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

iscsi

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the iSCSI service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the iSCSI service.

ldap

Name	Type	Description
ad_domain	string	This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with `servers` during POST.
base_dn	string	Specifies the default base DN for all searches.
bind_dn	string	Specifies the user that binds to the LDAP servers. SVM API supports anonymous binding. For Simple and SASL LDAP binding, use the LDAP API endpoint.
enabled	boolean	Enable LDAP? Setting to true creates a configuration if not already created.
restrict_discovery_to_site	boolean	Specifies whether or not LDAP server discovery is restricted to site-scope.
servers	array[string]	

ndmp

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NDMP service. If it is false, only the cluster administrator can manage the service.

nfs

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the NFS service. If it is false, only the cluster administrator can manage the service.

Name	Type	Description
enabled	boolean	If allowed, setting to true enables the NFS service.

nis

Name	Type	Description
_links	_links	
domain	string	The NIS domain to which this configuration belongs.
enabled	boolean	Enable NIS? Setting to true creates a configuration if not already created.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

nsswitch

Name service switch configuration

Name	Type	Description
group	array[string]	Group sources
hosts	array[string]	Host sources
namemap	array[string]	NameMap sources
netgroup	array[string]	NetGroup sources
passwd	array[string]	Password sources

nvme

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NVMe service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the NVMe service.

qos_adaptive_policy_group_template

This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.

Name	Type	Description
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy

This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.

Name	Type	Description
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy_group_template

This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.

Name	Type	Description
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

ip_info

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6
netmask	string	Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length.

network_route_for_svm

Name	Type	Description
destination	ip_info	IP information
gateway	string	The IP address of the gateway router leading to the destination.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

s3

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether or not to enable S3. Setting this value to true creates a service if one is not yet created.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server. By default, HTTPS is enabled on the S3 server.
name	string	Specifies the name of the S3 server. A server name length can range from 1 to 253 characters and can only contain the following combination of characters 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443.

snapmirror

Specifies attributes for SVM DR protection.

Name	Type	Description
is_protected	boolean	Specifies whether the SVM is a SnapMirror source SVM, using SnapMirror to protect its data.
protected_consistency_group_count	integer	Specifies the number of SVM DR protected consistency groups in the SVM.
protected_volumes_count	integer	Specifies the number of SVM DR protected volumes in the SVM.

snapshot_policy

This is a reference to the snapshot policy.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

storage

Name	Type	Description
allocated	integer	Total size of the volumes in SVM, in bytes.
available	integer	Currently available storage capacity in SVM, in bytes.
limit	integer	Maximum storage permitted on a single SVM, in bytes.
limit_threshold_alert	integer	Indicates at what percentage of storage capacity an alert message is sent. The default value is 90.
limit_threshold_exceeded	boolean	Indicates whether the total storage capacity exceeds the alert percentage.

Name	Type	Description
used_percentage	integer	The percentage of storage capacity used.

svm

Name	Type	Description
_links	_links	
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.

Name	Type	Description
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.
certificate	certificate	Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.
cifs	cifs	
comment	string	Comment
dns	dns	
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.

Name	Type	Description
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM
ipspace	ipspace	Either the UUID or name may be supplied on input.
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
ldap	ldap	
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	
nis	nis	
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.

Name	Type	Description
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.
qos_policy	qos_policy	This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.
state	string	SVM State
storage	storage	

Name	Type	Description
subtype	string	SVM subtype. The SVM subtype sync_destination is created automatically when an SVM of subtype sync_source is created on the source MetroCluster cluster. A POST request with sync_destination as SVM subtype is invalid. SVM of subtype data_engine cannot be explicitly created by the admin and most management changes are not allowed on it.
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create and provision an SVM

POST `/svm/svms`

Introduced In: 9.6

Creates and provisions an SVM. If no IPspace is provided, then the SVM is created on the `Default` IPspace.

- The number of parallel SVMs that can be created must not be greater than five.
- If a sixth SVM POST request is issued, the following error message is generated: "Maximum allowed SVM jobs exceeded. Wait for the existing SVM jobs to complete and try again."

Required properties

- `name` - Name of the SVM to be created.

Recommended optional properties

- `ipspace.name` or `ipspace.uuid` - IPspace of the SVM
- `is_space_reporting_logical` - Logical Space Reporting parameter of the SVM
- `is_space_enforcement_logical` - Logical Space Enforcement parameter of the SVM
- `ip_interfaces` - If provided, the following fields are required:
- `ip_interfaces.name` - Name of the interface
- `ip_interfaces.ip.address` - IP address
- `ip_interfaces.ip.netmask` - Netmask length or IP address
- `ip_interfaces.location.broadcast_domain.uuid` or `ip_interfaces.location.broadcast_domain.name` - Broadcast domain name or UUID belonging to the same IPspace of the SVM.
- `ip_interfaces.location.home_port.name` - Home port name
- `ip_interfaces.location.home_port.uuid` - Home port uuid
- `subnet.uuid` or `subnet.name` - Either name or UUID of the subnet to create.
- `routes` - If provided, the following field is required:
  - `routes.gateway` - Gateway IP address
- `cifs` - If provided, interfaces, routes and DNS must be provided. The following fields are also required:
  - `cifs.name` - Name of the CIFS server to be created for the SVM.
  - `cifs.ad_domain.fqdn` - Fully qualified domain name
  - `cifs.ad_domain.user` - Administrator username
  - `cifs.ad_domain.password` - User password
- `ldap` - If provided, the following fields are required:
  - `ldap.servers` or `ldap.ad_domain` - LDAP server list or Active Directory domain
  - `ldap.bind_dn` - Bind DN
  - `ldap.base_dn` - Base DN
- `nis` - If provided, the following fields are required:
  - `nis.servers` - NIS servers
  - `nis.domain` - NIS domain

- `dns` - If provided, the following fields are required:
  - `dns.servers` - Name servers
  - `dns.domains` - Domains
- `fc_interfaces` - If provided, the following fields are required:
  - `fc_interfaces.name` - Fibre Channel interface name
  - `fc_interfaces.data_protocol` - Fibre Channel interface data protocol
  - `fc_interfaces.location.port.uuid` or `fc_interfaces.location.port.name` and `fc_interfaces.location.port.node.name` - Either port UUID or port name and node name together must be provided.
- `s3` - If provided, the following field should also be specified:
  - <code>s3.name</code> - Name of the S3 server. If <code>s3.name' is not specified while </code>s3.enabled` is set to 'true', the S3 server will be created with the default name '<svm.name>_S3Server'.</svm.name>
  - `s3.port` - S3 server listener port.
  - `s3.secure_port` - S3 server listener port for HTTPS.
  - `s3.is_http_enabled` - S3 server connections over HTTP.
  - `s3.is_https_enabled` - S3 server connections over HTTPS.
  - `s3.certificate.name` - S3 server certificate name. This is required if the S3 server runs over HTTPS.
  - `s3.certificate.uuid` - S3 server certificate UUID. This is required if the S3 server runs over HTTPS.
- `auto_enable_analytics` - Auto-enable file system analytics on new volumes created in the SVM.
- `auto_enable_activity_tracking` - Auto-enable volume activity-tracking on new volumes created in the SVM.
- `storage.limit` - Maximum storage permitted on a single SVM.
- `storage.limit_threshold_alert` - At what percentage of storage capacity, alert message needs to be sent.

Default property values

If not specified in POST, the following default property values are assigned:

- `language` - *C.UTF-8*
- `ipspace.name` - *Default*
- `snapshot_policy.name` - *Default*
- `subtype` - *Default* (*sync-source* if MetroCluster configuration)
- `anti_ransomware_default_volume_state` - *disabled*
- `qos_adaptive_policy_group_template` - *extreme* (if using a platform with disaggregated storage and neither qos_policy_group_template nor qos_adaptive_policy_group_template are provided)

Related ONTAP commands

- `vserver create`
- `vserver add-aggregates`
- `network interface create`
- `network route create`
- `vserver services name-service dns create`
- `vserver nfs create`
- `vserver services name-service ldap client create`
- `vserver cifs create`
- `vserver services name-service nis-domain create`
- `vserver iscsi create`
- `vserver nvme create`
- `vserver fcp create`
- `vserver services name-service ns-switch create`
- `vserver object-store-server create`
- `vserver add-protocols`
- `vserver remove-protocols`

Examples

- Creates an SVM with default "snapshot_policy".

```
POST "/api/svm/svms" '{"name":"testVs",
"snapshot_policy":{"name":"default"}}'
```

- Creates an SVM and configures NFS, CIFS, and S3.

```
POST "/api/svm/svms" '{"name":"testVs", "nfs":{"enabled":"true"},
"cifs":{"enabled":"true"}, "s3":{"enabled":"true"}}'
```

- Creates an SVM and configures NVMe.

```
POST "/api/svm/svms" '{"name":"testVs", "nvme":{"enabled":"true"}}'
```

- Creates an SVM and configures LDAP.

```
POST "/api/svm/svms" '{"name":"testVs",
"snapshot_policy":{"name":"default"},
"ldap":{"servers":["10.140.101.1","10.140.101.2"],
"ad_domain":"abc.com", "base_dn":"dc=netapp,dc=com",
"bind_dn":"dc=netapp,dc=com"}}'
```

- Creates an SVM and configures NIS.

```
POST "/api/svm/svms" '{"name":"testVs",
"snapshot_policy":{"name":"default"}, "nis":{"enabled":"true",
"domain":"def.com","servers":["10.224.223.130", "10.224.223.131"]}}'
```

- Creates an SVM and configures DNS.

```
POST "/api/svm/svms" '{"name":"testVs",
"snapshot_policy":{"name":"default"},
"dns":{"domains":["abc.com","def.com"], "servers":["10.224.223.130",
"10.224.223.131"]}}'
```

- Creates an SVM and configures a LIF.

```
POST "/api/svm/svms" '{"name":"testVs", "ip_interfaces":
[{"name":"lif1", "ip":{"address":"10.10.10.7", "netmask":
"255.255.255.0"}, "location":{"broadcast_domain":{"name":"bd1"},
"home_node":{"name":"node1"}}, "service_policy": "default-
management"}]}'
```

- Creates an SVM and configures a LIF with IPV6 address.

```
POST "/api/svm/svms" '{"name":"testVs", "ip_interfaces":
[{"name":"lif2",
"ip":{"address":"fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b",
"netmask":"24"}, "location":{"broadcast_domain":{"name":"bd1"},
"home_node":{"name":"node1"}}, "service_policy": "default-
management"}]}'
```

- Creates an SVM and configures CIFS.

```
POST "/api/svm/svms" '{"name":"testVs", "cifs":{"name":"CIFDOC",
"ad_domain":{"fqdn":"abc.def.com", "organizational_unit":"CN=Computers",
"user":"cif_admin", "password":"abc123"}},
"ip_interfaces":[{"name":"lif1", "ip":{"address":"10.10.10.7",
"netmask": "255.255.255.0"},
"location":{"broadcast_domain":{"name":"bd1"},
"home_node":{"name":"node1"}}, "service_policy": "default-
management"}],"routes": [{"destination": {"address": "0.0.0.0",
"netmask": "0"}, "gateway": "10.10.10.7"}],
"dns":{"domains":["abc.def.com", "def.com"],
"servers":["10.224.223.130", "10.224.223.131"]}}'
```

- Creates an SVM with an S3 server enabled and configured.

```
POST "/api/svm/svms" '{"name":"svm5", "s3":{"name":"s3-server-1",
"enabled":true, "allowed":true, "is_http_enabled": true,
"is_https_enabled":false}}'
```

- Creates an SVM and disallows NVMe service for the SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "nvme":{"allowed":"false"}}'
```

- Creates an SVM, allows and configures the NFS service for the SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "nfs":{"allowed":"true",
"enabled":true}}'
```

- Create an SVM and set the max volume limit for the SVM.

```
POST "/api/svm/svms/" '{"name":"testVs", "max_volumes":"200"}'
```

- Creates an SVM and disallows the NDMP service for the SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "ndmp":{"allowed":"false"}}'
```

- Creates an SVM and specifies whether file system analytics is enabled on all newly created volumes in the SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "auto_enable_analytics":true}}'
```

- Creates an SVM and specifies whether volume_activity_tracking is enabled on all newly created volumes in the SVM.

```
POST "/api/svm/svms" '{"name":"testVs",
"auto_enable_activity_tracking":true}}'
```

- Creates an SVM and specifies whether file system analytics is enabled on all newly created volumes in the SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "auto_enable_analytics":true}}'
```

- Creates an SVM and specifies the maximum storage limit for a single SVM.

```
POST "/api/svm/svms" '{"name":"testVs", "storage": {"limit":"4GB"}}'
```

- Creates an SVM and specifies at what percentage of storage capacity an alert message is sent. Default value is 90.

```
POST "/api/svm/svms" '{"name":"testVs", "storage": {"limit":"20GB",
"limit_threshold_alert":"95"}}'
```

- Creates an SVM and specifies the QoS policy group template to be assigned to the SVM.

```
POST "/api/svm/svms" '{"name":"testVs",
"qos_policy_group_template":{"name":"performance-fixed"}}'
```

- Creates an SVM and specifies the QoS adaptive policy group template to be assigned to the SVM.

```
POST "/api/svm/svms" '{"name":"testVs",
"qos_adaptive_policy_group_template":{"name":"performance"}}'
```

Learn more

- DOC /svm/svms

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.

Name	Type	Description
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.

Name	Type	Description
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.
cifs	cifs	
comment	string	Comment
dns	dns	
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM
ipspace	ipspace	Either the UUID or name may be supplied on input.
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.

Name	Type	Description
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
ldap	ldap	
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	
nis	nis	
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.

Name	Type	Description
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
routes	array[network_route_for_svm]	Optional array of routes for the SVM
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.
storage	storage	
subtype	string	SVM subtype. The SVM subtype sync_destination is created automatically when an SVM of subtype sync_source is created on the source MetroCluster cluster. A POST request with sync_destination as SVM subtype is invalid. SVM of subtype data_engine cannot be explicitly created by the admin and most management changes are not allowed on it.
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

Example request


```
{
  "aggregates": [
    {
      "available_size": 10156560384,
      "name": "aggr1",
      "snaplock_type": "string",
      "state": "string",
      "type": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "anti_ransomware_auto_switch_minimum_incoming_data": "string",
  "anti_ransomware_default_volume_state": "string",
  "anti_ransomware_incoming_write_threshold": "string",
  "anti_ransomware_incoming_write_threshold_percent": "string",
  "cifs": {
    "ad_domain": {
      "default_site": "string",
      "fqdn": "example.com",
      "organizational_unit": "string",
      "password": "string",
      "user": "string"
    },
    "auth-style": "domain",
    "domain_workgroup": "string",
    "name": "CIFS1",
    "workgroup": "workgrp1"
  },
  "comment": "string",
  "dns": {
    "domains": [
      "example.com",
      "example2.example3.com"
    ],
    "servers": [
      "10.224.65.20",
      "2001:db08:a0b:12f0::1"
    ]
  },
  "fc_interfaces": [
    {
      "data_protocol": "string",
      "location": {
        "port": {
```

```
          "name": "0a",
          "node": {
            "name": "node1"
          },
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      },
      "name": "lif1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "ip_interfaces": [
    {
      "ip": {
        "address": "10.10.10.7",
        "netmask": "24"
      },
      "location": {
        "broadcast_domain": {
          "name": "bd1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "home_node": {
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "home_port": {
          "name": "e1b",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        }
      },
      "name": "lif1",
      "service_policy": "string",
      "services": [
        "data_nfs"
      ],
      "subnet": {
        "name": "subnet1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
```

```
  },
  "language": "c.utf_8",
  "ldap": {
    "ad_domain": "string",
    "base_dn": "string",
    "bind_dn": "string",
    "servers": [
      "string"
    ]
  },
  "max_volumes": "string",
  "name": "svm1",
  "nis": {
    "domain": "string",
    "servers": [
      "string"
    ]
  },
  "nsswitch": {
    "group": [
      "string"
    ],
    "hosts": [
      "string"
    ],
    "namemap": [
      "string"
    ],
    "netgroup": [
      "string"
    ],
    "passwd": [
      "string"
    ]
  },
  "number_of_volumes_in_recovery_queue": 0,
  "qos_adaptive_policy_group_template": {
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
```

```
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "qos_policy_group_template": {
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "routes": [
    {
      "destination": {
        "address": "10.10.10.7",
```

```
        "netmask": "24"
      },
      "gateway": "10.1.1.1"
    }
  ],
  "s3": {
    "certificate": {
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "default_unix_user": "string",
    "default_win_user": "string",
    "name": "s3-server-1"
  },
  "snapmirror": {
    "protected_consistency_group_count": 0,
    "protected_volumes_count": 0
  },
  "snapshot_policy": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "storage": {
    "allocated": 0,
    "available": 0,
    "used_percentage": 0
  },
  "subtype": "string",
  "total_volume_size_in_recovery_queue": 0,
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
```


Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error codes	Description
2621580	Cannot specify options other than SVM name, comment and ipspace for a Vserver that is being configured as the destination for SVM DR.
2621634	"sync-source" SVM can only be created in a MetroCluster configuration.
2621657	"sync-destination" SVM can only be created by the system.
13434884	Cannot create an SVM because of incorrect fields.
13434885	Non-UTF8 language(s) not supported.
13434888	IPspace UUID and IPspace name mismatch.
13434889	Internal Error. Wait and retry.
13434894	Maximum allowed SVM jobs exceeded. Wait for the existing SVM jobs to complete and try again.

Error codes	Description
13434908	Invalid SVM name. The name is already in use by another SVM, IPSpace or cluster.
13434909	Internal Error. Failed to identify the aggregate to host SVM root volume.
13434910	Internal Error. Failed to allocate new SVM ID.
13434911	Invalid SVM name. Maximum supported length is 41 if SVM is of type \"sync-source\", otherwise 47.
13434912	Failed to find IPspace.
13434913	Internal error: Failed to check if an SVM create operation is in progress. Contact technical support for assistance.
13434914	Request to create the root volume of the SVM failed because there is not enough space in specified aggregate.
13434915	Failed to unlock the SVM because SVM create or delete job is in progress. Wait a few minutes, and then try the command again.
13434916	SVM is in the process of being created. Wait a few minutes, and then try the command again.
13434917	SVM creation successful.
13434918	IPspace name not provided for creating an SVM.
458753	Destination and gateway must belong to the same address family.
23724038	Invalid source for the provided ns-switch database.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

aggregates

Name	Type	Description
available_size	integer	Space available, in bytes.
name	string	
snaplock_type	string	SnapLock type.
state	string	Aggregate state.
type	string	Type of aggregate.
uuid	string	

event_log

Name	Type	Description
is_enabled_on_new_file_extension_seen	boolean	Specifies whether to send an EMS when a new file extension is discovered.
is_enabled_on_snapshot_copy_creation	boolean	Specifies whether to send an EMS when a snapshot is created.

arw_vserver

Anti-ransomware related information for the SVM.

Name	Type	Description
event_log	event_log	

certificate

Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server.
password	string	The account password used to add this CIFS server to the Active Directory. This is not audited. Valid in POST only.
user	string	The user account used to add this CIFS server to the Active Directory. Valid in POST only.

cifs

Name	Type	Description
ad_domain	ad_domain	
allowed	boolean	If this is set to true, an SVM administrator can manage the CIFS service. If it is false, only the cluster administrator can manage the service.
auth-style	string	Authentication type.

Name	Type	Description
domain_workgroup	string	The NetBIOS name of the domain or workgroup associated with the CIFS server.
enabled	boolean	If allowed, setting to true enables the CIFS service.
name	string	The NetBIOS name of the CIFS server.
workgroup	string	The workgroup name.

dns

Name	Type	Description
domains	array[string]	A list of DNS domains. Domain names have the following requirements: • The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_". • The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9. • The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9. • The top level domain must contain only the following characters: A through Z, a through z. • The system reserves the following names:"all", "local", and "localhost".
servers	array[string]	The list of IP addresses of the DNS servers. Addresses can be either IPv4 or IPv6 addresses.

node

The node on which the FC port is located.

Name	Type	Description
name	string	The name of the node on which the FC port is located.

fc_port_reference

An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

Name	Type	Description
name	string	The name of the FC port.
node	node	The node on which the FC port is located.
uuid	string	The unique identifier of the FC port.

location

The location of the Fibre Channel interface is defined by the location of its port.

Name	Type	Description
port	fc_port_reference	An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

fc_interface_svm

Name	Type	Description
data_protocol	string	The data protocol for which the Fibre Channel interface is configured.
location	location	The location of the Fibre Channel interface is defined by the location of its port.
name	string	The name of the Fibre Channel interface.

Name	Type	Description
uuid	string	The unique identifier of the Fibre Channel interface.

fcp

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the FCP service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the FCP service.

ip

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	Input as netmask length (16) or IPv4 mask (255.255.0.0).

broadcast_domain

Broadcast domain UUID along with a readable name.

Name	Type	Description
name	string	Name of the broadcast domain, scoped to its IPspace
uuid	string	Broadcast domain UUID

home_node

Name	Type	Description
name	string	
uuid	string	

port_svm

Name	Type	Description
name	string	
uuid	string	

location

Home_node is optional.

Name	Type	Description
broadcast_domain	broadcast_domain	Broadcast domain UUID along with a readable name.
home_node	home_node	
home_port	port_svm	

ip_subnet_reference

A named subnet. Either UUID or name can be supplied on input.

Name	Type	Description
name	string	The name of the subnet. If only the name is provided, the IPspace scope must be provided by the object this object is embedded in.
uuid	string	The UUID that uniquely identifies the subnet.

ip_interface_svm

Interface parameters. Name and home_node are optional.

Name	Type	Description
ip	ip	IP information
location	location	Home_node is optional.
name	string	The name of the interface (optional).
service_policy	string	Built-in service policies for SVMs.

Name	Type	Description
services	array[string]	The services associated with the interface.
subnet	ip_subnet_reference	A named subnet. Either UUID or name can be supplied on input.
uuid	string	The UUID that uniquely identifies the interface.

ipspace

Either the UUID or name may be supplied on input.

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

iscsi

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the iSCSI service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the iSCSI service.

ldap

Name	Type	Description
ad_domain	string	This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with `servers` during POST.
base_dn	string	Specifies the default base DN for all searches.

Name	Type	Description
bind_dn	string	Specifies the user that binds to the LDAP servers. SVM API supports anonymous binding. For Simple and SASL LDAP binding, use the LDAP API endpoint.
enabled	boolean	Enable LDAP? Setting to true creates a configuration if not already created.
restrict_discovery_to_site	boolean	Specifies whether or not LDAP server discovery is restricted to site-scope.
servers	array[string]	

ndmp

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NDMP service. If it is false, only the cluster administrator can manage the service.

nfs

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NFS service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the NFS service.

nis

Name	Type	Description
domain	string	The NIS domain to which this configuration belongs.

Name	Type	Description
enabled	boolean	Enable NIS? Setting to true creates a configuration if not already created.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

nsswitch

Name service switch configuration

Name	Type	Description
group	array[string]	Group sources
hosts	array[string]	Host sources
namemap	array[string]	NameMap sources
netgroup	array[string]	NetGroup sources
passwd	array[string]	Password sources

nvme

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NVMe service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the NVMe service.

qos_adaptive_policy_group_template

This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy

This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy_group_template

This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

ip_info

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length.

network_route_for_svm

Name	Type	Description
destination	ip_info	IP information
gateway	string	The IP address of the gateway router leading to the destination.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

s3

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether or not to enable S3. Setting this value to true creates a service if one is not yet created.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server. By default, HTTP is disabled on the S3 server.

Name	Type	Description
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server. By default, HTTPS is enabled on the S3 server.
name	string	Specifies the name of the S3 server. A server name length can range from 1 to 253 characters and can only contain the following combination of characters 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443.

snapmirror

Specifies attributes for SVM DR protection.

Name	Type	Description
is_protected	boolean	Specifies whether the SVM is a SnapMirror source SVM, using SnapMirror to protect its data.
protected_consistency_group_count	integer	Specifies the number of SVM DR protected consistency groups in the SVM.
protected_volumes_count	integer	Specifies the number of SVM DR protected volumes in the SVM.

snapshot_policy

This is a reference to the snapshot policy.

Name	Type	Description
name	string	
uuid	string	

storage

Name	Type	Description
allocated	integer	Total size of the volumes in SVM, in bytes.
available	integer	Currently available storage capacity in SVM, in bytes.
limit	integer	Maximum storage permitted on a single SVM, in bytes.
limit_threshold_alert	integer	Indicates at what percentage of storage capacity an alert message is sent. The default value is 90.
limit_threshold_exceeded	boolean	Indicates whether the total storage capacity exceeds the alert percentage.
used_percentage	integer	The percentage of storage capacity used.

svm

Name	Type	Description
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.

Name	Type	Description
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.

Name	Type	Description
cifs	cifs	
comment	string	Comment
dns	dns	
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM
ipspace	ipspace	Either the UUID or name may be supplied on input.
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
ldap	ldap	
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	
nis	nis	

Name	Type	Description
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
routes	array[network_route_for_svm]	Optional array of routes for the SVM
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.
storage	storage	

Name	Type	Description
subtype	string	SVM subtype. The SVM subtype sync_destination is created automatically when an SVM of subtype sync_source is created on the source MetroCluster cluster. A POST request with sync_destination as SVM subtype is invalid. SVM of subtype data_engine cannot be explicitly created by the admin and most management changes are not allowed on it.
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete an SVM

DELETE `/svm/svms/{uuid}`

Introduced In: 9.6

Deletes an SVM. As a prerequisite, SVM objects must be deleted first. SnapMirror relationships must be deleted and data volumes must be offline and deleted.

- The number of parallel SVMs that can be created must not be greater than five.
- If a sixth SVM POST request is issued, the following error message is generated: "Maximum allowed SVM jobs exceeded. Wait for the existing SVM jobs to complete and try again."

Related ONTAP commands

- `vserver delete`

Example

Deleting an individual SVM in the cluster.

```
DELETE "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
```

Learn more

- DOC /svm/svms

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Filter by UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```


Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error codes	Description
13434894	Maximum allowed SVM jobs exceeded. Wait and retry.
2621525	SVM cannot be deleted as it is associated with an Active Directory configured CIFS server. Delete the CIFS server using "cifs delete" and retry the operation.

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

job_link

Name	Type	Description
_links	_links	
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve SVM properties

GET `/svm/svms/{uuid}`

Introduced In: 9.6

Retrieves the properties for an individual SVM. This includes protocol configurations such as CIFS and NFS, export policies, name service configurations, and network services.

Important notes

- The SVM object includes a large set of fields and can be expensive to retrieve.
- REST APIs only expose a data SVM as an SVM.

Expensive properties

There is an added computational cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See Requesting specific fields to learn more.

- `snapmirror.*`

Example

Retrieving an individual SVM in the cluster

```
GET "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
```

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Filter by UUID
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.

Name	Type	Description
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.

Name	Type	Description
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.
certificate	certificate	Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.
cifs	cifs	
comment	string	Comment
dns	dns	
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM

Name	Type	Description
ipspace	ipspace	Either the UUID or name may be supplied on input.
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
ldap	ldap	
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	
nis	nis	
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.

Name	Type	Description
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.
qos_policy	qos_policy	This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.
state	string	SVM State
storage	storage	

Name	Type	Description
subtype	string	SVM subtype. The SVM subtype sync_destination is created automatically when an SVM of subtype sync_source is created on the source MetroCluster cluster. A POST request with sync_destination as SVM subtype is invalid. SVM of subtype data_engine cannot be explicitly created by the admin and most management changes are not allowed on it.
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "aggregates": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "available_size": 10156560384,
      "name": "aggr1",
      "snaplock_type": "string",
      "state": "string",
      "type": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "anti_ransomware_auto_switch_minimum_incoming_data": "string",
  "anti_ransomware_default_volume_state": "string",
  "anti_ransomware_incoming_write_threshold": "string",
  "anti_ransomware_incoming_write_threshold_percent": "string",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "cifs": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "ad_domain": {
      "default_site": "string",
      "fqdn": "example.com",
      "organizational_unit": "string"
```

```
    },
    "auth-style": "domain",
    "domain_workgroup": "string",
    "name": "CIFS1",
    "workgroup": "workgrp1"
  },
  "comment": "string",
  "dns": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "domains": [
      "example.com",
      "example2.example3.com"
    ],
    "servers": [
      "10.224.65.20",
      "2001:db08:a0b:12f0::1"
    ]
  },
  "fc_interfaces": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "data_protocol": "string",
      "name": "lif1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "fcp": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "ip_interfaces": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
```

```
        }
      },
      "ip": {
        "address": "10.10.10.7"
      },
      "name": "lif1",
      "services": [
        "data_nfs"
      ],
      "subnet": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "subnet1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "iscsi": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "language": "c.utf_8",
  "ldap": {
    "ad_domain": "string",
    "base_dn": "string",
    "bind_dn": "string",
    "servers": [
      "string"
    ]
  },
```

```
  "max_volumes": "string",
  "name": "svm1",
  "nfs": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "nis": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "domain": "string",
    "servers": [
      "string"
    ]
  },
  "nsswitch": {
    "group": [
      "string"
    ],
    "hosts": [
      "string"
    ],
    "namemap": [
      "string"
    ],
    "netgroup": [
      "string"
    ],
    "passwd": [
      "string"
    ]
  },
  "number_of_volumes_in_recovery_queue": 0,
  "nvme": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
  "qos_adaptive_policy_group_template": {
```

```
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "qos_policy": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
```

```
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "qos_policy_group_template": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
```

```
  "s3": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "default_unix_user": "string",
    "default_win_user": "string",
    "name": "s3-server-1"
  },
  "snapmirror": {
    "protected_consistency_group_count": 0,
    "protected_volumes_count": 0
  },
  "snapshot_policy": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "state": "running",
  "storage": {
    "allocated": 0,
    "available": 0,
    "used_percentage": 0
  },
  "subtype": "string",
  "total_volume_size_in_recovery_queue": 0,
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error codes	Description
262188	Field "top_metric" was specified twice (to "iops.read" and "throughput.read").

Name	Type	Description
error	returned_error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

aggregates

Name	Type	Description
_links	_links	
available_size	integer	Space available, in bytes.
name	string	
snaplock_type	string	SnapLock type.
state	string	Aggregate state.
type	string	Type of aggregate.
uuid	string	

event_log

Name	Type	Description
is_enabled_on_new_file_extension_seen	boolean	Specifies whether to send an EMS when a new file extension is discovered.
is_enabled_on_snapshot_copy_creation	boolean	Specifies whether to send an EMS when a snapshot is created.

arw_vserver

Anti-ransomware related information for the SVM.

Name	Type	Description
event_log	event_log	

certificate

Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server.

cifs

Name	Type	Description
_links	_links	
ad_domain	ad_domain	
allowed	boolean	If this is set to true, an SVM administrator can manage the CIFS service. If it is false, only the cluster administrator can manage the service.
auth-style	string	Authentication type.
domain_workgroup	string	The NetBIOS name of the domain or workgroup associated with the CIFS server.

Name	Type	Description
enabled	boolean	If allowed, setting to true enables the CIFS service.
name	string	The NetBIOS name of the CIFS server.
workgroup	string	The workgroup name.

dns

Name	Type	Description
_links	_links	
domains	array[string]	A list of DNS domains. Domain names have the following requirements: • The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_". • The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9. • The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9. • The top level domain must contain only the following characters: A through Z, a through z. • The system reserves the following names:"all", "local", and "localhost".
servers	array[string]	The list of IP addresses of the DNS servers. Addresses can be either IPv4 or IPv6 addresses.

node

The node on which the FC port is located.

Name	Type	Description
name	string	The name of the node on which the FC port is located.

fc_port_reference

An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

Name	Type	Description
_links	_links	
name	string	The name of the FC port.
node	node	The node on which the FC port is located.
uuid	string	The unique identifier of the FC port.

location

The location of the Fibre Channel interface is defined by the location of its port.

Name	Type	Description
port	fc_port_reference	An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

fc_interface_svm

Name	Type	Description
_links	_links	
data_protocol	string	The data protocol for which the Fibre Channel interface is configured.
name	string	The name of the Fibre Channel interface.
uuid	string	The unique identifier of the Fibre Channel interface.

fcp

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the FCP service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the FCP service.

ip

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address

broadcast_domain

Broadcast domain UUID along with a readable name.

Name	Type	Description
_links	_links	
name	string	Name of the broadcast domain, scoped to its IPspace
uuid	string	Broadcast domain UUID

home_node

Name	Type	Description
_links	_links	
name	string	
uuid	string	

port_svm

Name	Type	Description
_links	_links	
name	string	

Name	Type	Description
uuid	string	

location

Home_node is optional.

Name	Type	Description
broadcast_domain	broadcast_domain	Broadcast domain UUID along with a readable name.
home_node	home_node	
home_port	port_svm	

ip_subnet_reference

A named subnet. Either UUID or name can be supplied on input.

Name	Type	Description
_links	_links	
name	string	The name of the subnet. If only the name is provided, the IPspace scope must be provided by the object this object is embedded in.
uuid	string	The UUID that uniquely identifies the subnet.

ip_interface_svm

Interface parameters. Name and home_node are optional.

Name	Type	Description
_links	_links	
ip	ip	IP information
name	string	The name of the interface (optional).
services	array[string]	The services associated with the interface.
subnet	ip_subnet_reference	A named subnet. Either UUID or name can be supplied on input.

Name	Type	Description
uuid	string	The UUID that uniquely identifies the interface.

ipspace

Either the UUID or name may be supplied on input.

Name	Type	Description
_links	_links	
name	string	IPspace name
uuid	string	IPspace UUID

iscsi

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the iSCSI service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the iSCSI service.

ldap

Name	Type	Description
ad_domain	string	This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with `servers` during POST.
base_dn	string	Specifies the default base DN for all searches.

Name	Type	Description
bind_dn	string	Specifies the user that binds to the LDAP servers. SVM API supports anonymous binding. For Simple and SASL LDAP binding, use the LDAP API endpoint.
enabled	boolean	Enable LDAP? Setting to true creates a configuration if not already created.
restrict_discovery_to_site	boolean	Specifies whether or not LDAP server discovery is restricted to site-scope.
servers	array[string]	

ndmp

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NDMP service. If it is false, only the cluster administrator can manage the service.

nfs

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the NFS service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the NFS service.

nis

Name	Type	Description
_links	_links	
domain	string	The NIS domain to which this configuration belongs.

Name	Type	Description
enabled	boolean	Enable NIS? Setting to true creates a configuration if not already created.
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

nsswitch

Name service switch configuration

Name	Type	Description
group	array[string]	Group sources
hosts	array[string]	Host sources
namemap	array[string]	NameMap sources
netgroup	array[string]	NetGroup sources
passwd	array[string]	Password sources

nvme

Available for GET, POST, and PATCH requests.

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the NVMe service. If it is false, only the cluster administrator can manage the service.
enabled	boolean	If allowed, setting to true enables the NVMe service.

qos_adaptive_policy_group_template

This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy

This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy_group_template

This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).

Name	Type	Description
_links	_links	
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.

Name	Type	Description
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

ip_info

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address
family	string	IPv4 or IPv6
netmask	string	Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length.

network_route_for_svm

Name	Type	Description
destination	ip_info	IP information
gateway	string	The IP address of the gateway router leading to the destination.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
_links	_links	
name	string	Certificate name
uuid	string	Certificate UUID

s3

Name	Type	Description
_links	_links	
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service.
certificate	certificate	Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
default_unix_user	string	Specifies the default UNIX user for NAS Access.
default_win_user	string	Specifies the default Windows user for NAS Access.
enabled	boolean	Specifies whether or not to enable S3. Setting this value to true creates a service if one is not yet created.
is_http_enabled	boolean	Specifies whether HTTP is enabled on the S3 server. By default, HTTP is disabled on the S3 server.
is_https_enabled	boolean	Specifies whether HTTPS is enabled on the S3 server. By default, HTTPS is enabled on the S3 server.
name	string	Specifies the name of the S3 server. A server name length can range from 1 to 253 characters and can only contain the following combination of characters 0-9, A-Z, a-z, ".", and "-".
port	integer	Specifies the HTTP listener port for the S3 server. By default, HTTP is enabled on port 80.
secure_port	integer	Specifies the HTTPS listener port for the S3 server. By default, HTTPS is enabled on port 443.

snapmirror

Specifies attributes for SVM DR protection.

Name	Type	Description
is_protected	boolean	Specifies whether the SVM is a SnapMirror source SVM, using SnapMirror to protect its data.

Name	Type	Description
protected_consistency_group_count	integer	Specifies the number of SVM DR protected consistency groups in the SVM.
protected_volumes_count	integer	Specifies the number of SVM DR protected volumes in the SVM.

snapshot_policy

This is a reference to the snapshot policy.

Name	Type	Description
_links	_links	
name	string	
uuid	string	

storage

Name	Type	Description
allocated	integer	Total size of the volumes in SVM, in bytes.
available	integer	Currently available storage capacity in SVM, in bytes.
limit	integer	Maximum storage permitted on a single SVM, in bytes.
limit_threshold_alert	integer	Indicates at what percentage of storage capacity an alert message is sent. The default value is 90.
limit_threshold_exceeded	boolean	Indicates whether the total storage capacity exceeds the alert percentage.
used_percentage	integer	The percentage of storage capacity used.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update SVM properties

PATCH `/svm/svms/{uuid}`

Introduced In: 9.6

Updates one or more of the following properties of an individual SVM: SVM name, SVM default volume language code, SVM comment, and SVM state.

Related ONTAP commands

- `vserver modify`
- `vserver rename`
- `vserver start`
- `vserver stop`
- `security ssl modify`
- `vserver add-protocols`
- `vserver remove-protocols`

Examples

1. Stops an SVM and updates the "comment" field for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"state":"stopped", "comment":"This SVM is stopped."}'
```

1. Starts an SVM and updates the "comment" field for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"state":"running", "comment":"This SVM is running."}'
```

1. Updates the "language" field for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"language":"en.UTF-8"}'
```

1. Updates the "name" field for an SVM or renames the SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"name":"svm_new"}'
```

1. Updates the aggregates for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":["{"name":aggr1"},{"name":"aggr2"},{"name":"aggr3"}]}'
```

1. Updates the snapshot policy for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"snapshot_policy":{"name":"custom1"}}'
```

1. Updates the TLS certificate for an individual SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"certificate":{"uuid":"1cd8a442-86d1-11e0-ae1c-123478563412"}}'
```

1. Updates the QoS policy for the SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"qos_policy_group":{"name":"qpolicy1"}}'
```

1. Allows NFS protocol which was previously disallowed for the SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"nfs":{"allowed":"true"}}'
```

1. Updates the max volume limit for the SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"max_volumes":"200"}'
```

1. Updates whether file system analytics is enabled on all newly created volumes in the SVM.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"auto_enable_analytics":"true"}'
```

1. Updates whether volume activity tracking is enabled on all newly created volumes in the SVM.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"auto_enable_activity_tracking":"true"}'
```

1. Updates the QoS adaptive policy group template for the SVM.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"qos_adaptive_policy_group_template":{"name":"aqpolicy1"}}'
```

1. Updates the maximum storage permitted on a single SVM.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"storage":{"limit":"40GB"}}'
```

1. Updates the percentage of storage capacity at which an alert message is sent.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"storage":{"limit":"400MB", "limit_threshold_alert":"98"}}'
```

1. Updates the QoS policy group template for the SVM.

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"qos_policy_group_template":{"name":"policy1"}}'
```

1. Updates the S3 protocol that was previously disallowed for the SVM

```
  PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"s3":{"allowed":"true"}}'
```

Learn more

- DOC /svm/svms

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Filter by UUID
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.

Name	Type	Description
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.
certificate	certificate	Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.
cifs	cifs	
comment	string	Comment
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM

Name	Type	Description
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.

Name	Type	Description
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.
qos_policy	qos_policy	This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.
state	string	SVM State
storage	storage	
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

Example request


```
{
  "aggregates": [
    {
      "available_size": 10156560384,
      "name": "aggr1",
      "snaplock_type": "string",
      "state": "string",
      "type": "string",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "anti_ransomware_auto_switch_minimum_incoming_data": "string",
  "anti_ransomware_default_volume_state": "string",
  "anti_ransomware_incoming_write_threshold": "string",
  "anti_ransomware_incoming_write_threshold_percent": "string",
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "cifs": {
    "auth-style": "domain",
    "domain_workgroup": "string",
    "enabled": true,
    "workgroup": "workgrp1"
  },
  "comment": "string",
  "fc_interfaces": [
    {
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ],
  "fcp": {
    "enabled": true
  },
  "ip_interfaces": [
    {
      "services": [
        "data_nfs"
      ],
      "subnet": {
        "name": "subnet1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
```

```
    }
  ],
  "iscsi": {
    "enabled": true
  },
  "language": "c.utf_8",
  "max_volumes": "string",
  "name": "svm1",
  "nfs": {
    "enabled": true
  },
  "nsswitch": {
    "group": [
      "string"
    ],
    "hosts": [
      "string"
    ],
    "namemap": [
      "string"
    ],
    "netgroup": [
      "string"
    ],
    "passwd": [
      "string"
    ]
  },
  "number_of_volumes_in_recovery_queue": 0,
  "nvme": {
    "enabled": true
  },
  "qos_adaptive_policy_group_template": {
    "max_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
```

```
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "min_throughput_iops": 2000,
      "min_throughput_mbps": 500,
      "name": "performance",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "qos_policy": {
      "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "max_throughput_iops": 10000,
      "max_throughput_mbps": 500,
      "min_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
        "1000IOPS,25MB/s"
      ],
      "min_throughput_iops": 2000,
      "min_throughput_mbps": 500,
      "name": "performance",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "qos_policy_group_template": {
      "max_throughput": [
        "900KB/s",
        "500MB/s",
        "120GB/s",
        "5000IOPS",
        "5000IOPS,500KB/s",
        "2500IOPS,100MB/s",
```

```
      "1000IOPS,25MB/s"
    ],
    "max_throughput_iops": 10000,
    "max_throughput_mbps": 500,
    "min_throughput": [
      "900KB/s",
      "500MB/s",
      "120GB/s",
      "5000IOPS",
      "5000IOPS,500KB/s",
      "2500IOPS,100MB/s",
      "1000IOPS,25MB/s"
    ],
    "min_throughput_iops": 2000,
    "min_throughput_mbps": 500,
    "name": "performance",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "s3": {
    "enabled": true,
    "is_http_enabled": true,
    "is_https_enabled": true
  },
  "snapmirror": {
    "protected_consistency_group_count": 0,
    "protected_volumes_count": 0
  },
  "snapshot_policy": {
    "name": "default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "state": "running",
  "storage": {
    "allocated": 0,
    "available": 0,
    "used_percentage": 0
  },
  "total_volume_size_in_recovery_queue": 0,
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
```


Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response


```
{
  "job": {
    "uuid": "string"
  }
}
```


Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error codes	Description
13434880	Failed to modify SVM parameters.
13434881	Failed to rename SVM.
13434883	SVM parameters except name modified successfully.
13434885	Non-UTF8 language(s) not supported.
13434886	Invalid snapshot policy.
13434902	Modification of NSSwitch parameters failed for the SVM.
13434906	Operation not supported for an SVM of type sync-destination.
12451843	Certificate does not exist.
13434908	Invalid SVM name. The name is already in use by another SVM, IPSpace or cluster.

Error codes	Description
13434916	SVM is in the process of being created. Wait a few minutes, and then try the command again.
13434915	Failed to unlock the SVM because SVM create or delete job is in progress. Wait a few minutes, and then try the command again.
13434911	Invalid SVM name. Maximum supported length is 41 if SVM is of type \"sync-source\", otherwise 47.
262179	Unexpected argument "storage_limit".
23724038	Invalid source for the provided ns-switch database.
2621779	Operation not supported for an SVM of type data-engine.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

aggregates

Name	Type	Description
available_size	integer	Space available, in bytes.
name	string	
snaplock_type	string	SnapLock type.
state	string	Aggregate state.
type	string	Type of aggregate.
uuid	string	

event_log

Name	Type	Description
is_enabled_on_new_file_extension_seen	boolean	Specifies whether to send an EMS when a new file extension is discovered.
is_enabled_on_snapshot_copy_creation	boolean	Specifies whether to send an EMS when a snapshot is created.

arw_vserver

Anti-ransomware related information for the SVM.

Name	Type	Description
event_log	event_log	

certificate

Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.

cifs

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the CIFS service. If it is false, only the cluster administrator can manage the service.
auth-style	string	Authentication type.
domain_workgroup	string	The NetBIOS name of the domain or workgroup associated with the CIFS server.
workgroup	string	The workgroup name.

dns

Name	Type	Description
domains	array[string]	A list of DNS domains. Domain names have the following requirements: • The name must contain only the following characters: A through Z, a through z, 0 through 9, ".", "-" or "_". • The first character of each label, delimited by ".", must be one of the following characters: A through Z or a through z or 0 through 9. • The last character of each label, delimited by ".", must be one of the following characters: A through Z, a through z, or 0 through 9. • The top level domain must contain only the following characters: A through Z, a through z. • The system reserves the following names:"all", "local", and "localhost".
servers	array[string]	The list of IP addresses of the DNS servers. Addresses can be either IPv4 or IPv6 addresses.

node

The node on which the FC port is located.

Name	Type	Description
name	string	The name of the node on which the FC port is located.

fc_port_reference

An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

Name	Type	Description
name	string	The name of the FC port.

Name	Type	Description
node	node	The node on which the FC port is located.
uuid	string	The unique identifier of the FC port.

location

The location of the Fibre Channel interface is defined by the location of its port.

Name	Type	Description
port	fc_port_reference	An FC port is the physical port of an FC adapter on a cluster node that can be connected to an FC network.

fc_interface_svm

Name	Type	Description
uuid	string	The unique identifier of the Fibre Channel interface.

fcp

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the FCP service. If it is false, only the cluster administrator can manage the service.

ip

IP information

broadcast_domain

Broadcast domain UUID along with a readable name.

Name	Type	Description
name	string	Name of the broadcast domain, scoped to its IPspace

Name	Type	Description
uuid	string	Broadcast domain UUID

home_node

Name	Type	Description
name	string	
uuid	string	

port_svm

Name	Type	Description
name	string	
uuid	string	

location

Home_node is optional.

Name	Type	Description
broadcast_domain	broadcast_domain	Broadcast domain UUID along with a readable name.
home_node	home_node	
home_port	port_svm	

ip_subnet_reference

A named subnet. Either UUID or name can be supplied on input.

Name	Type	Description
name	string	The name of the subnet. If only the name is provided, the IPspace scope must be provided by the object this object is embedded in.
uuid	string	The UUID that uniquely identifies the subnet.

ip_interface_svm

Interface parameters. Name and home_node are optional.

Name	Type	Description
ip	ip	IP information
services	array[string]	The services associated with the interface.
subnet	ip_subnet_reference	A named subnet. Either UUID or name can be supplied on input.
uuid	string	The UUID that uniquely identifies the interface.

ipspace

Either the UUID or name may be supplied on input.

Name	Type	Description
name	string	IPspace name
uuid	string	IPspace UUID

iscsi

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the iSCSI service. If it is false, only the cluster administrator can manage the service.

ldap

Name	Type	Description
ad_domain	string	This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with `servers` during POST.
base_dn	string	Specifies the default base DN for all searches.

Name	Type	Description
bind_dn	string	Specifies the user that binds to the LDAP servers. SVM API supports anonymous binding. For Simple and SASL LDAP binding, use the LDAP API endpoint.
enabled	boolean	Enable LDAP? Setting to true creates a configuration if not already created.
restrict_discovery_to_site	boolean	Specifies whether or not LDAP server discovery is restricted to site-scope.
servers	array[string]	

ndmp

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NDMP service. If it is false, only the cluster administrator can manage the service.

nfs

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NFS service. If it is false, only the cluster administrator can manage the service.

nis

Name	Type	Description
domain	string	The NIS domain to which this configuration belongs.
enabled	boolean	Enable NIS? Setting to true creates a configuration if not already created.

Name	Type	Description
servers	array[string]	A list of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

nsswitch

Name service switch configuration

Name	Type	Description
group	array[string]	Group sources
hosts	array[string]	Host sources
namemap	array[string]	NameMap sources
netgroup	array[string]	NetGroup sources
passwd	array[string]	Password sources

nvme

Available for GET, POST, and PATCH requests.

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the NVMe service. If it is false, only the cluster administrator can manage the service.

qos_adaptive_policy_group_template

This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy

This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

qos_policy_group_template

This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).

Name	Type	Description
max_throughput	string	Specifies the maximum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either max_throughput_mbps or max_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.
max_throughput_iops	integer	Specifies the maximum throughput in IOPS, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
max_throughput_mbps	integer	Specifies the maximum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when max_throughput is set during POST or PATCH.
min_throughput	string	Specifies the minimum throughput in Kilobytes per sec, Megabytes per sec or Gigabytes per sec along with or without IOPS. 0 means none.Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when either min_throughput_mbps or min_throughput_iops are set during POST or PATCH. During GET, the returned value is rounded to the largest unit with a value greater than 1.

Name	Type	Description
min_throughput_iops	integer	Specifies the minimum throughput in IOPS, 0 means none. Setting "min_throughput" is supported on AFF platforms only, unless FabricPool tiering policies are set. This is mutually exclusive with name and UUID during POST and PATCH. This cannot be set when min_throughput is set during POST or PATCH.
min_throughput_mbps	integer	Specifies the minimum throughput in Megabytes per sec, 0 means none. This is mutually exclusive with name and UUID during POST and PATCH.This cannot be set when min_throughput is set during POST or PATCH.
name	string	The QoS policy group name. This is mutually exclusive with UUID and other QoS attributes during POST and PATCH.
uuid	string	The QoS policy group UUID. This is mutually exclusive with name and other QoS attributes during POST and PATCH.

ip_info

IP information

Name	Type	Description
address	string	IPv4 or IPv6 address
netmask	string	Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length.

network_route_for_svm

Name	Type	Description
destination	ip_info	IP information
gateway	string	The IP address of the gateway router leading to the destination.

certificate

Specifies the certificate that will be used for creating HTTPS connections to the S3 server.

Name	Type	Description
name	string	Certificate name
uuid	string	Certificate UUID

s3

Name	Type	Description
allowed	boolean	If this is set to true, an SVM administrator can manage the S3 service. If it is false, only the cluster administrator can manage the service.

snapmirror

Specifies attributes for SVM DR protection.

Name	Type	Description
is_protected	boolean	Specifies whether the SVM is a SnapMirror source SVM, using SnapMirror to protect its data.
protected_consistency_group_count	integer	Specifies the number of SVM DR protected consistency groups in the SVM.
protected_volumes_count	integer	Specifies the number of SVM DR protected volumes in the SVM.

snapshot_policy

This is a reference to the snapshot policy.

Name	Type	Description
name	string	
uuid	string	

storage

Name	Type	Description
allocated	integer	Total size of the volumes in SVM, in bytes.
available	integer	Currently available storage capacity in SVM, in bytes.
limit	integer	Maximum storage permitted on a single SVM, in bytes.
limit_threshold_alert	integer	Indicates at what percentage of storage capacity an alert message is sent. The default value is 90.
limit_threshold_exceeded	boolean	Indicates whether the total storage capacity exceeds the alert percentage.
used_percentage	integer	The percentage of storage capacity used.

svm

Name	Type	Description
aggregates	array[aggregates]	List of allowed aggregates for SVM volumes. An administrator is allowed to create volumes on these aggregates.
aggregates_delegated	boolean	This property is true when the administrator has delegated the aggregates for the SVM volumes.
anti_ransomware	arw_vserver	Anti-ransomware related information for the SVM.

Name	Type	Description
anti_ransomware_auto_switch_duration_without_new_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that no new file-extensions are observed in the volume in recent time. This parameter optionally specifies the recent time duration (in days) to be considered during which no new file-extension should be observed in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_from_learning_to_enabled	boolean	This property specifies whether anti-ransomware state of the volumes in this SVM are automatically switched by the system from “learning” (dry-run) to “enabled” (active) state after sufficient learning. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_file_count	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have a minimum file count in “learning” state. This parameter optionally specifies the minimum number of newly created files in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_file_extension	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have minimum number of file extensions in “learning” state. This parameter optionally specifies the minimum number of new file extensions in “learning” state in a given volume to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_auto_switch_minimum_incoming_data	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_auto_switch_minimum_learning_period	integer	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should be in “learning” state for sufficient time period. This parameter optionally specifies the minimum number of days a given volume should be in “learning” state to automatically switch the anti-ransomware state from “learning” to “enabled”. This field will no longer be supported in a future release.
anti_ransomware_default_volume_state	string	Specifies the default anti-ransomware state of the volumes in the SVM. The default "anti_ransomware_default_volume_state" property is disabled for POST operations. If this value is "disabled", anti-ransomware protection is disabled by default on the new volumes that are created in the SVM. If this value is "dry_run", anti-ransomware protection is in learning mode by default on the new volumes that are created in the SVM. When the anti-ransomware license is not present, this property is ignored and volumes will be created with the "disabled" state. This value "dry_run" will no longer be supported in a future release.

Name	Type	Description
anti_ransomware_incoming_write_threshold	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in GB) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field is no longer supported.
anti_ransomware_incoming_write_threshold_percent	string	One of the many conditions to be satisfied to automatically switch the anti-ransomware state of the volumes in this SVM from “learning” (dry-run) to “enabled” is that the volume should have sufficient data ingested to do the learning. This parameter optionally specifies the minimum amount of data (in percentage) to be written to a given volume during the learning period to automatically switch the anti-ransomware state from “learning” to “enabled”. The amount of data considered as ingested also includes the data that is deleted or overwritten after ingestion. This field will no longer be supported in a future release.
auto_enable_activity_tracking	boolean	Specifies whether volume activity tracking is automatically enabled on volumes that are created in the SVM.
auto_enable_analytics	boolean	Specifies whether file system analytics is automatically enabled on volumes that are created in the SVM.

Name	Type	Description
certificate	certificate	Support for this field will be removed in a future release. Please use /svm/svms/{svm.uuid}/web for this field. Certificate for incoming TLS connection requests.
cifs	cifs	
comment	string	Comment
fc_interfaces	array[fc_interface_svm]	FC Interface for the SVM
fcp	fcp	Available for GET, POST, and PATCH requests.
ip_interfaces	array[ip_interface_svm]	IP interfaces for the SVM
is_space_enforcement_logical	boolean	Indicates whether logical space enforcement for the SVM is enabled.
is_space_reporting_logical	boolean	Indicates whether logical space reporting for the SVM is enabled.
iscsi	iscsi	Available for GET, POST, and PATCH requests.
language	string	Default volume language code. UTF-8 encoded languages are valid in POST or PATCH. Non UTF-8 language encodings are for backward compatibility and are not valid input for POST and PATCH requests.
max_volumes	string	This property is used by cluster administrator to specify the limit on maximum number of volumes allowed in the SVM. The value can be either the string "unlimited" or a number.
name	string	The name of the SVM.
ndmp	ndmp	
nfs	nfs	

Name	Type	Description
nsswitch	nsswitch	Name service switch configuration
number_of_volumes_in_recovery_queue	integer	Number of volumes in the recovery queue.
nvme	nvme	Available for GET, POST, and PATCH requests.
qos_adaptive_policy_group_template	qos_adaptive_policy_group_template	This optionally specifies which QoS adaptive policy group to apply to the SVM as a template. This policy group will then be assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs) that adjust based on the volume allocated space or used space.
qos_policy	qos_policy	This optionally specifies which QoS policy group to apply to the Vserver. This policy group defines measurable service level objectives (SLOs) that apply to the storage objects with which the policy group is associated.
qos_policy_group_template	qos_policy_group_template	This optionally specifies which QoS non-shared policy group to apply to the SVM as a template. This policy group is then assigned to volumes created or rehosted into this SVM. This policy group defines measurable service level objectives (SLOs) and Service Level Agreements (SLAs).
s3	s3	
snapmirror	snapmirror	Specifies attributes for SVM DR protection.
snapshot_policy	snapshot_policy	This is a reference to the snapshot policy.

Name	Type	Description
state	string	SVM State
storage	storage	
total_volume_size_in_recovery_queue	integer	Sum of the sizes of the volumes in the recovery queue.
uuid	string	The unique identifier of the SVM.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Copyright information

Trademark information